System and Method for Communicating A Secure Unidirectional Response Message

(A-70561/RMA)

WE CLAIM:

1. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure unidirectional response message, the program module including instructions for:

A. extracting, by a Client who is sending a secure response message to the Entity in order to respond to a message from the Entity, the Entity's public key and matching destination address of the Entity from a trusted storage means;

B. extracting, by the Client, the Client's public and private key and certificate chain from a trusted source or storage means;

C. using, the extracted Client's public and private key and certificate chain information along with the previously extracted Entity's destination address to create a secure unidirectional message to the Entity using the a secure unidirectional message protocol, a data portion of the Client's message containing a Resource Tag that was included in the message received from the Entity to which this message is a response; and

D. verifying, by the Entity, the Client's certificate chain.

2. A hardware architecture neutral and operating system neutral and network transport neutral method for secure unidirectional response message using less software code and network bandwidth than conventional systems, said method comprising the steps of:

A. extracting, by a Client who is sending a secure response message to the Entity in order to respond to a message from the Entity, the Entity's public key and matching destination address of the Entity from a trusted storage means;

B. extracting, by the Client, the Client's public and private key and certificate chain from a trusted source or storage means;

C. using, the extracted Client's public and private key and certificate chain information along with the previously extracted Entity's destination address to create a secure unidirectional message to the Entity using the a secure unidirectional message protocol, a data portion of the Client's message containing a Resource Tag that was included in the message received from the Entity to which this message is a response; and

D. verifying, by the Entity, the Client's certificate chain.

3. The method in Claim 2, further comprising: E. performing, by the Entity, an appropriate application-level action for the received response message.

4. The method in Claim 2, wherein the Entity's public key comprises an RSA or RSA-based key.

5. The method in Claim 2, wherein the matching destination address comprises an e-mail address.

6. The method in Claim 2, wherein the public key and matching destination address have been verified previously using a digital signature (verified with a trusted public key) or cryptographic checksum (verified with a trusted key derived from a Master Key or Session Key or Message Key).

7. The method in Claim 2, wherein the trusted source or storage means comprises data from a normal e-mail message, a non-secured web page, or a secured web page, or combination thereof.

8. The method in Claim 2, wherein the web page is secured by one of the set consisting or SSL, PCT, or TLS.

9. The method in Claim 2, wherein the trusted source or storage means comprises data received from communicating with a Server via a secure session.

10. The method in Claim 2, wherein the Client's keys and certificate chain are fixed values shared by more than one Client system, and the Entity authenticates the Client based on this Resource Tag.

11. The method in Claim 2, wherein the Client's keys and certificate chain are unique to this client, and the Entity authenticates the Client using this unique certificate and/or using a Resource Tag which was included in the message received from the Entity to which this session is a response.

12. The method in Claim 2, wherein the Entity authenticates the Client using the certificate and/or using a Resource Tag which was included in the message received from the Entity to which this session is a response.

13. The method in Claim 2, wherein said verifying by the Entity, further includes optionally verifying the Resource Tag that is included in the Data portion of the received message.

14. The method in Claim 2, wherein the secure unidirectional message protocol comprises using the Signed-Inside-Enveloped-Data cryptographic primitive.

15. The method in claim 2, wherein said Entity comprises a Merchant.

16. A method for communicating a secure unidirectional response message from a Client that is sending a secure response message to the Entity in order to respond to a message from the Entity, said method comprising the steps of:

extracting, by the Client, information including the Entity's public key and matching destination address and the Client's public and private key and certificate chain from one or more trusted source; and

using, by the Client, the extracted information to create a secure unidirectional message to the Entity using the a secure unidirectional message protocol, a data portion of the secure unidirectional message containing a resource tag that was included in the message received from the Entity to which the secure unidirectional message is a response.

17. The method in claim 16, further comprising sending the secure unidirectional message to the entity.

18. The method in claim 17, further comprising verifying, by the Entity, the Client's certificate chain.

19. The method of claim 16, wherein the trusted source or storage means comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root public key.

20. The method of claim 2, wherein the trusted source or storage means comprises a Compact Certificate as explained earlier, or chain of Compact Certificates leading to a trusted root public key.